Question 1

Why is NAT not needed in IPv6?

- Because IPv6 has integrated security, there is no need to hide the IPv6 addresses of internal networks.
- Any host or user can get a public IPv6 network address because the number of available IPv6 addresses is extremely large.
- The problems that are induced by NAT applications are solved because the IPv6 header improves packet handling by intermediate routers.
- The end-to-end connectivity problems that are caused by NAT are solved because the number of routes increases with the number of nodes that are connected to the Internet.

Explanation: The large number of public IPv6 addresses eliminates the need for NAT. Sites from the largest enterprises to single households can get public IPv6 network addresses. This avoids some of the NAT-induced application problems that are experienced by applications that require end-to-end connectivity.

Question 2

What is one advantage that the IPv6 simplified header offers over IPv4?

- smaller-sized header
- little requirement for processing checksums
- smaller-sized source and destination IP addresses
- efficient packet handling

Explanation: The IPv6 simplified header offers several advantages over IPv4:

- Better routing efficiency and efficient packet handling for performance and forwarding-rate scalability
- No requirement for processing checksums
- Simplified and more efficient extension header mechanisms (as opposed to the IPv4 Options field)
- A Flow Label field for per-flow processing with no need to open the transport inner packet to identify the various traffic flows

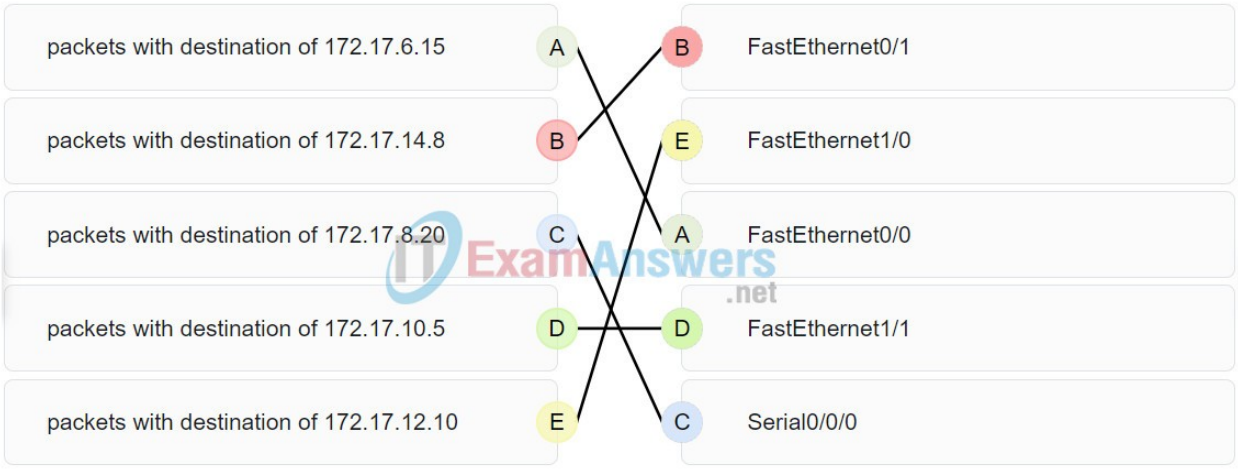
Question 3

Refer to the exhibit. Match the packets with their destination IP address to the exiting interfaces on the router. (Not all targets are used.)

```
<output omitted>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.0.0 is directly connected, Serial0/0/0
     172.17.0.0/24 is subnetted, 4 subnets
O       172.17.6.0 [110/2] via 192.168.3.4, 00:10:41, FastEthernet0/0
O       172.17.10.0 [110/2] via 192.168.5.2, 00:09:52, FastEthernet1/1
O       172.17.12.0 [110/2] via 192.168.4.2, 00:12:23, FastEthernet1/0
C       172.17.14.0 is directly connected, FastEthernet0/1
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet1/0
C    192.168.5.0/24 is directly connected, FastEthernet1/1
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```



Place the options in the following order:

packets with destination of 172.17.6.15	FastEthernet0/0
packets with destination of 172.17.14.8	FastEthernet0/1
packets with destination of 172.17.12.10	FastEthernet1/0
packets with destination of 172.17.10.5	FastEthernet1/1
packets with destination of 172.17.8.20	Serial0/0/0

Explanation: Packets with a destination of 172.17.6.15 are forwarded through Fa0/0. Packets with a destination of 172.17.10.5 are forwarded through Fa1/1. Packets with a destination of 172.17.12.10 are forwarded through Fa1/0. Packets with a destination of 172.17.14.8 are forwarded through Fa0/1. Because network 172.17.8.0 has no entry in the routing table, it will take the gateway of last resort, which means that packets with a destination of 172.17.8.20 are forwarded through Serial0/0/0. Because a gateway of last resort exists, no packets will be dropped.

Question 4

What information does the loopback test provide?

- **The TCP/IP stack on the device is working correctly.**
- The device has end-to-end connectivity.
- DHCP is working correctly.
- The Ethernet cable is working correctly.

- The device has the correct IP address on the network.

Explanation: Because the loopback test sends packets back to the host device, it does not provide information about network connectivity to other hosts. The loopback test verifies that the host NIC, drivers, and TCP/IP stack are functioning.

Question 5

When transporting data from real-time applications, such as streaming audio and video, which field in the IPv6 header can be used to inform the routers and switches to maintain the same path for the packets in the same conversation?

- Next Header
- Flow Label
- Traffic Class
- Differentiated Services

Explanation: The Flow Label in IPv6 header is a 20-bit field that provides a special service for real-time applications. This field can be used to inform routers and switches to maintain the same path for the packet flow so that packets will not be reordered.

Question 6

A computer can access devices on the same network but cannot access devices on other networks. What is the probable cause of this problem?

- The cable is not connected properly to the NIC.
- The computer has an invalid IP address.
- The computer has an incorrect subnet mask.
- The computer has an invalid default gateway address.

Explanation: The default gateway is the address of the device a host uses to access the Internet or another network. If the default gateway is missing or incorrect, that host will not be able to communicate outside the local network. Because the host can access other hosts on the local network, the network cable and the other parts of the IP configuration are working.

Question 7

How do hosts ensure that their packets are directed to the correct network destination?

- They have to keep their own local routing table that contains a route to the loopback interface, a local network route, and a remote default route.
- They always direct their packets to the default gateway, which will be responsible for the packet delivery.
- They search in their own local routing table for a route to the network destination address and pass this information to the default gateway.
- They send a query packet to the default gateway asking for the best route.

Explanation: Hosts must maintain their own local routing table to ensure that network layer packets are directed to the correct destination network. This local table typically contains a route to the loopback interface, a route to the network that the host is connected to, and a local default route, which represents the route that packets must take to reach all remote network addresses.

Question 8

What IPv4 header field identifies the upper layer protocol carried in the packet?

- Protocol
- Identification
- Version
- Differentiated Services

Explanation: It is the Protocol field in the IP header that identifies the upper-layer protocol the packet is carrying. The Version field identifies the IP version. The Differential Services field is used for setting packet priority. The Identification field is used to reorder fragmented packets.

Question 9

Which field in the IPv4 header is used to prevent a packet from traversing a network endlessly?

- Time-to-Live
- Sequence Number
- Acknowledgment Number
- Differentiated Services

Explanation: The value of the Time-to-Live (TTL) field in the IPv4 header is used to limit the lifetime of a packet. The sending host sets the initial TTL value; which is decreased by one each time the packet is processed by a router. If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) Time Exceeded message to the source IP address. The Differentiated Services (DS) field is used to determine the priority of each packet. Sequence Number and Acknowledgment Number are two fields in the TCP header.

Question 10

Which two types of IPv6 messages are used in place of ARP for address resolution?

- anycast
- broadcast

- echo reply
- echo request
- neighbor solicitation
- neighbor advertisement

Explanation: IPv6 does not use ARP. Instead, ICMPv6 neighbor discovery is used by sending neighbor solicitation and neighbor advertisement messages.

Question 11

Which destination address is used in an ARP request frame?

- 0.0.0.0
- 255.255.255.255
- FFFF.FFFF.FFFF
- AAAA.AAAA.AAAA
- the physical address of the destination host

Explanation: The purpose of an ARP request is to find the MAC address of the destination host on an Ethernet LAN. The ARP process sends a Layer 2 broadcast to all devices on the Ethernet LAN. The frame contains the IP address of the destination and the broadcast MAC address, FFFF.FFFF.FFFF. The host with the IP address that matches the IP address in the ARP request will reply with a unicast frame that includes the MAC address of the host. Thus the original sending host will obtain the destination IP and MAC address pair to continue the encapsulation process for data transmission.

Question 12

Under which two circumstances will a switch flood a frame out of every port except the port that the frame was received on? (Choose two.)

- The frame has the broadcast address as the destination address.
- The destination address is unknown to the switch.
- The source address in the frame header is the broadcast address.
- The source address in the frame is a multicast address.
- The destination address in the frame is a known unicast address.

Explanation: A switch will flood a frame out of every port, except the one that the frame was received from, under two circumstances. Either the frame has the broadcast address as the destination address, or the destination address is unknown to the switch.

Question 13

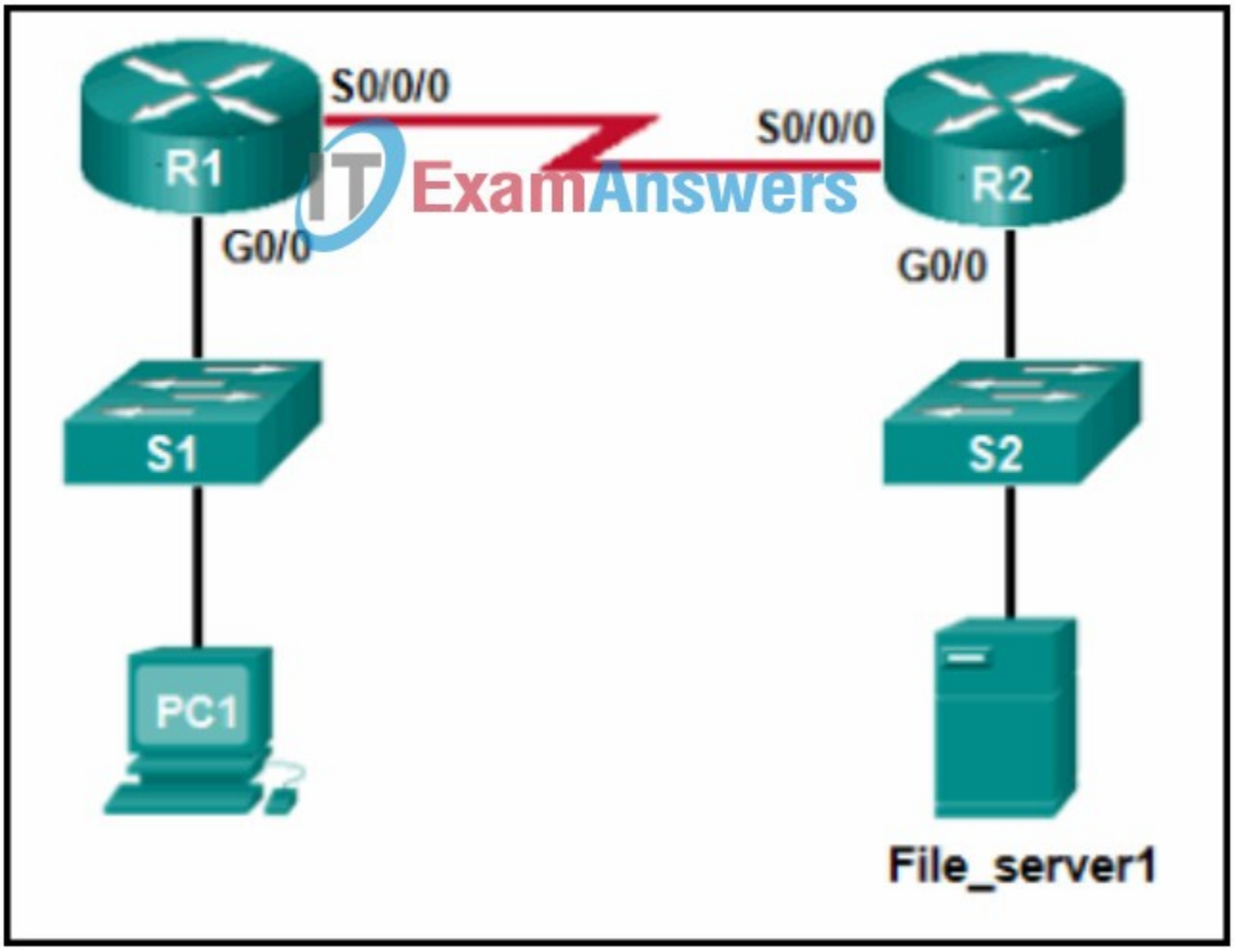
What important information is examined in the Ethernet frame header by a Layer 2 device in order to forward the data onward?

- source MAC address
- source IP address
- **destination MAC address**
- Ethernet type
- destination IP address

Explanation: The Layer 2 device, such as a switch, uses the destination MAC address to determine which path (interface or port) should be used to send the data onward to the destination device.

Question 14

Refer to the exhibit. PC1 attempts to connect to File_server1 and sends an ARP request to obtain a destination MAC address. Which MAC address will PC1 receive in the ARP reply?



- the MAC address of S1
- **the MAC address of the G0/0 interface on R1**
- the MAC address of the G0/0 interface on R2
- the MAC address of S2
- the MAC address of File_server1

Explanation: PC1 must have a MAC address to use as a destination Layer 2 address. PC1 will send an ARP request as a broadcast and R1 will send back an ARP reply with its G0/0 interface MAC address. PC1 can then forward the packet to the MAC address of the default gateway, R1.

Question 15

A network technician issues the arp -d * command on a PC after the router that is connected to the LAN is reconfigured. What is the result after this command is issued?

- The ARP cache is cleared.
- The current content of the ARP cache is displayed.
- The detailed information of the ARP cache is displayed.
- The ARP cache is synchronized with the router interface.

Explanation: Issuing the **arp –d *** command on a PC will clear the ARP cache content. This is helpful when a network technician wants to ensure the cache is populated with updated information.

Question 16

Where are IPv4 address to Layer 2 Ethernet address mappings maintained on a host computer?

- neighbor table
- ARP cache
- routing table
- MAC address table

Explanation: The ARP cache is used to store IPv4 addresses and the Ethernet physical addresses or MAC addresses to which the IPv4 addresses are mapped. Incorrect mappings of IP addresses to MAC addresses can result in loss of end-to-end connectivity.

Question 17

The global configuration command ip default-gateway 172.16.100.1 is applied to a switch. What is the effect of this command?

- The switch will have a management interface with the address 172.16.100.1.
- The switch can be remotely managed from a host on another network.
- The switch can communicate with other hosts on the 172.16.100.0 network.
- The switch is limited to sending and receiving frames to and from the gateway 172.16.100.1.

Explanation: A default gateway address is typically configured on all devices to allow them to communicate beyond just their local network.In a switch this is achieved using the command ip default-gateway <ip address>.

Question 18

A router boots and enters setup mode. What is the reason for this?

- The IOS image is corrupt.
- Cisco IOS is missing from flash memory.
- The configuration file is missing from NVRAM.
- The POST process has detected hardware failure.

Explanation: If a router cannot locate the startup-config file in NVRAM it will enter setup mode to allow the configuration to be entered from the console device.

Question 19

What happens when the transport input ssh command is entered on the switch vty lines?

- The SSH client on the switch is enabled.
- Communication between the switch and remote users is encrypted.
- The switch requires a username/password combination for remote access.
- The switch requires remote connections via a proprietary client software.

Explanation: The **transport input ssh** command when entered on the switch vty (virtual terminal lines) will encrypt all inbound controlled telnet connections.

Question 20

Match the phases to the functions during the boot up process of a Cisco router.

phase 2	✓ locate and load the Cisco IOS software
phase 3	✓ locate and load the startup configuration file
phase 1	✓ perform the POST and load the bootstrap program

IT ExamAnswers

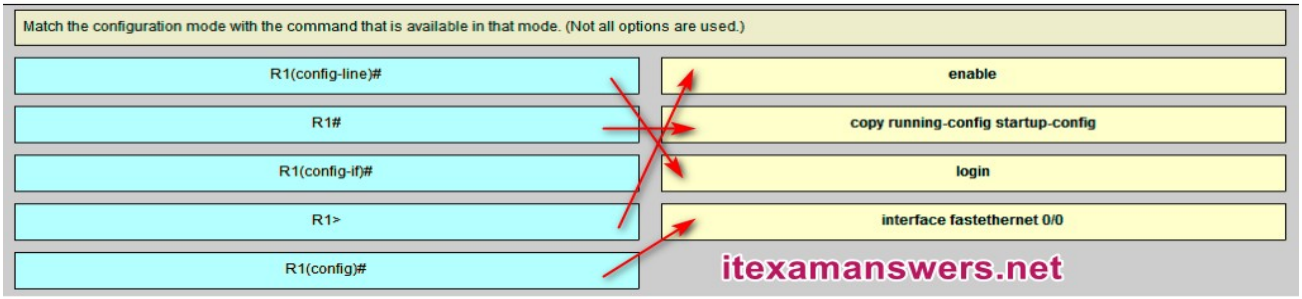
Explanation: Place the options in the following order:

phase 2	locate and load the Cisco IOS software
phase 3	locate and load the startup configuration file
phase 1	perform the POST and load the bootstrap program

Question 21

Match the configuration mode with the command that is available in that mode. (Not all options are used.)

Answer



Sort elements
R1> -> enable
R1# -> copy running-config startup-config
R1(config-line)# login
R1(config)# -> interface fastethernet 0/0
Explanation: At the **R1>** prompt, the **enable** command is entered. At the R1(config-line)# prompt, the **login** command is entered. At the R1# prompt, the **copy running-config startup-config** command is entered. At the R1(config)# prompt, the **interface fastethernet 0/0** command is entered.

Question 22

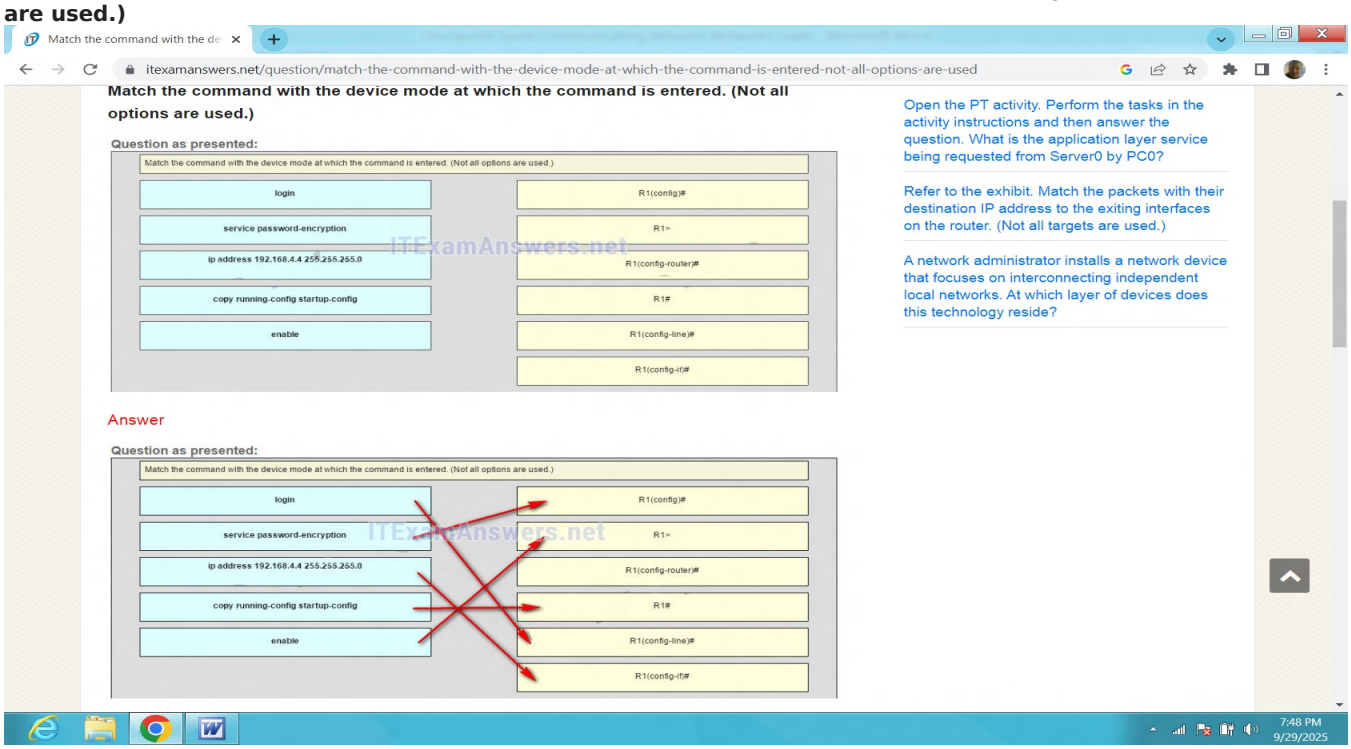
A new network administrator has been asked to enter a banner message on a Cisco device. What is the fastest way a network administrator could test whether the banner is properly configured?

- Reboot the device.
- Enter CTRL-Z at the privileged mode prompt.
- Exit global configuration mode.
- Power cycle the device.
- Exit privileged EXEC mode and press Enter.

Explanation: While at the privileged mode prompt such as Router#, type **exit, press Enter,** and the banner message appears. Power cycling a network device that has had the **banner motd** command issued will also display the banner message, but this is not a quick way to test the configuration.

Question 23

Match the command with the device mode at which the command is entered. (Not all options are used.)

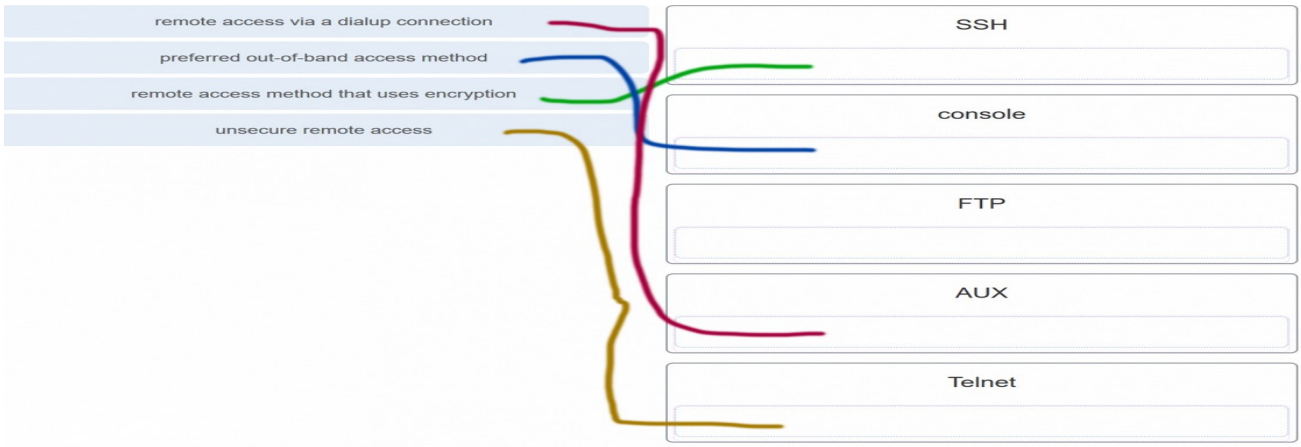


Answer

Explanation: The **enable** command is entered in R1> mode. The **login** command is entered in R1(config-line)# mode. The **copy running-config startup-config** command is entered in R1# mode. The **ip address 192.168.4.4 255.255.255.0** command is entered in R1(config-if)# mode. The **service password-encryption** command is entered in global configuration mode.

Question 24

A network administrator requires access to manage routers and switches locally and remotely. Match the description to the access method. (Not all options are used.)



Remote access via a dialup connection → AUX

Remote access method that used encryption → SSH

Preferred out-of-band access method → console

Unsecure remote access → Telnet

Explanation: Both the console and AUX ports can be used to directly connect to a Cisco network device for management purposes. However, it is more common to use the console port. The AUX port is more often used for remote access via a dial up connection. SSH and Telnet are both remote access methods that depend on an active network connection. SSH uses a stronger password authentication than Telnet uses and also uses encryption on transmitted data.

Question 25

Which three commands are used to set up secure access to a router through a connection to the console interface? (Choose three.)

- interface fastethernet 0/0
- line vty 0 4
- line console 0
- enable secret cisco
- login
- password cisco

Explanation:

The three commands needed to password protect the console port are as follows:

- **line console 0**
- **password cisco**
- **login**

The **interface fastethernet 0/0** command is commonly used to access the configuration mode used to apply specific parameters such as the IP address to the Fa0/0 port. The **line vty 0 4** command is used to access the configuration mode for Telnet. The0and 4 parameters specify ports 0 through 4, or a maximum of five simultaneous Telnet connections. The **enable secret** command is used to apply a password used on the router to access the privileged mode.

Question 26

```
PC>tracert www.cisco.com

Tracing route to 172.24.2.1 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      172.20.0.254
  2    0 ms      0 ms      0 ms      172.20.1.18
  3    1 ms      1 ms      1 ms      172.20.1.1
  4    2 ms      0 ms      1 ms      172.20.1.22
  5    2 ms      2 ms      2 ms      172.24.255.17
  6    2 ms      2 ms      3 ms      172.24.255.13
  7    2 ms      1 ms      2 ms      172.24.255.4
  8    3 ms      1 ms      1 ms      172.24.2.1

Trace complete.
```

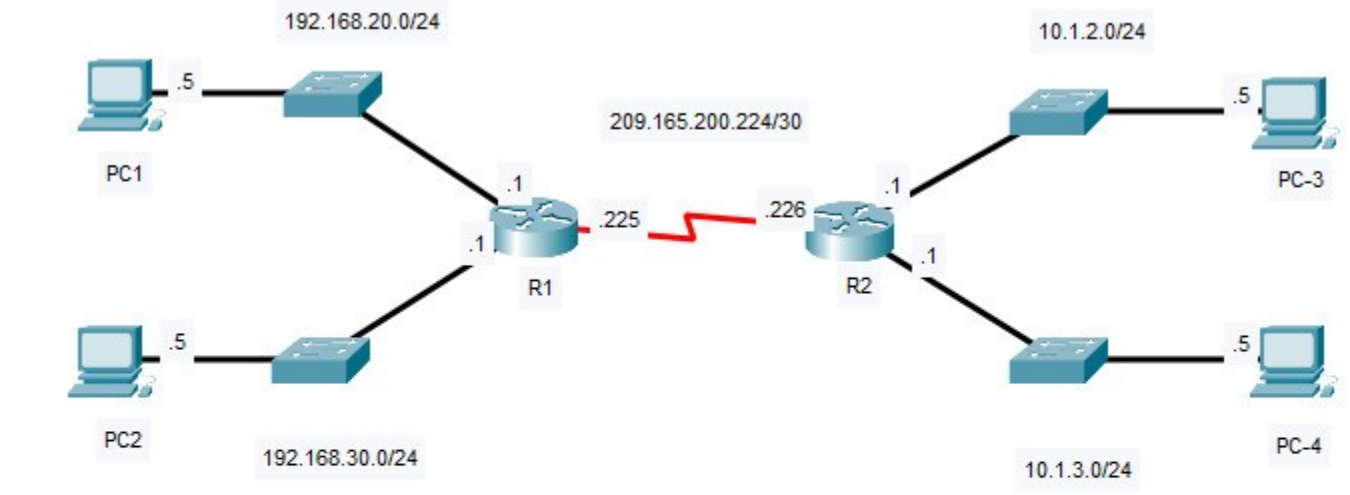
Refer to the exhibit. A user PC has successfully transmitted packets to http://www.cisco.com. Which IP address does the user PC target in order to forward its data off the local network?

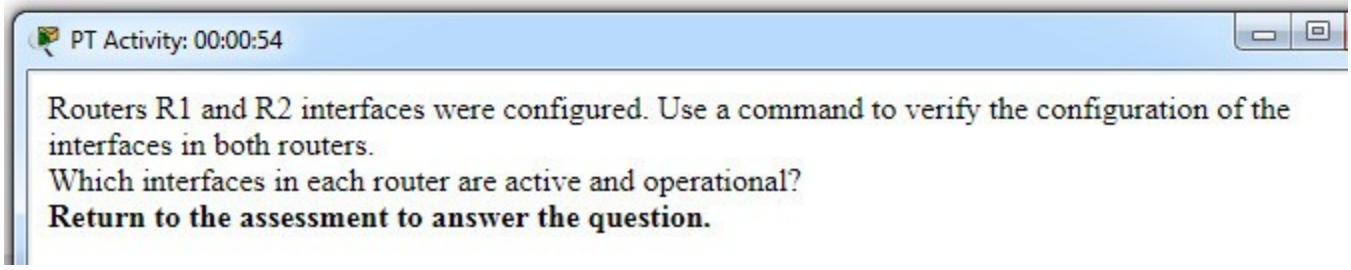
- 172.24.255.17
- 172.24.1.22
- 172.20.0.254
- 172.24.255.4
- 172.20.1.18

Question 27

Download PT Activity

Open the PT activity. Perform the tasks in the activity instructions and then answer the question.





Which interfaces in each router are active and operational?

- R1: G0/0 and S0/0/0
  R2: G0/0 and S0/0/0
- R1: G0/1 and S0/0/1
  R2: G0/0 and S0/0/1

- R1: G0/0 and S0/0/0
  R2: G0/1 and S0/0/0
- R1: G0/0 and S0/0/1
  R2: G0/1 and S0/0/1

Explanation: The command to use for this activity is **show ip interface brief** in each router. The active and operational interfaces are represented by the value “up” in the “Status” and “Protocol” columns. The interfaces in R1 with these characteristics are G0/0 and S0/0/0. In R2 they are G0/1 and S0/0/0.

Question 28

What are two potential network problems that can result from ARP operation? (Choose two.)

- Manually configuring static ARP associations could facilitate ARP poisoning or MAC address spoofing.
- On large networks with low bandwidth, multiple ARP broadcasts could cause data communication delays.
- Network attackers could manipulate MAC address and IP address mappings in ARP messages with the intent of intercepting network traffic.
- Large numbers of ARP request broadcasts could cause the host MAC address table to overflow and prevent the host from communicating on the network.
- Multiple ARP replies result in the switch MAC address table containing entries that match the MAC addresses of hosts that are connected to the relevant switch port.

Explanation: Large numbers of ARP broadcast messages could cause momentary data communications delays. Network attackers could manipulate MAC address and IP address mappings in ARP messages with the intent to intercept network traffic. ARP requests and replies cause entries to be made into the ARP table, not the MAC address table. ARP table overflows are very unlikely. Manually configuring static ARP associations is a way to prevent, not facilitate, ARP poisoning and MAC address spoofing. Multiple ARP replies resulting in the switch MAC address table containing entries that match the MAC addresses of connected nodes and are associated with the relevant switch port are required for normal switch frame forwarding operations. It is not an ARP caused network problem.

Question 29

What will happen if the default gateway address is incorrectly configured on a host?

- The host cannot communicate with other hosts in the local network.
- The switch will not forward packets initiated by the host.
- The host will have to use ARP to determine the correct address of the default gateway.
- The host cannot communicate with hosts in other networks.
- A ping from the host to 127.0.0.1 would not be successful.

Explanation: When a host needs to send a message to another host located on the same network, it can forward the message directly. However, when a host needs to send a message to a remote network, it must use the router, also known as the default gateway. This is because the data link frame address of the remote destination host cannot be used directly. Instead, the IP packet has to be sent to the router (default gateway) and the router will forward the packet toward its destination. Therefore, if the default gateway is incorrectly configured, the host can communicate with other hosts on the same network, but not with hosts on remote networks.

Question 30

What is the effect of using the Router# copy running-config startup-config command on a router?

- The contents of ROM will change.
- The contents of RAM will change.
- The contents of NVRAM will change.
- The contents of flash will change.

Explanation: The command **copy running-config startup-config** copies the running-configuration file from RAM into NVRAM and saves it as the startup-configuration file. Since NVRAM is none-volatile memory it will be able to retain the configuration details when the router is powered off.

Question 31

Which term describes a field in the IPv4 packet header that contains a 32-bit binary value associated with an interface on the sending device?

- source IPv4 address
- destination IPv4 address

- protocol
- TTL

Question 32

What property of ARP allows hosts on a LAN to send traffic to remote networks?

- Local hosts learn the MAC address of the default gateway.
- The destination MAC address FF-FF-FF-FF-FF-FF appears in the header of the Ethernet frame.
- The source MAC address appears in the header of the Ethernet frame.
- The port-to-MAC address table on a switch has the same entries as the ARP table on the switch.

Question 33

Refer to the exhibit. A network administrator is connecting a new host to the Manager LAN. The host needs to communicate with remote networks. What IP address would be configured as the default gateway on the new host?

```
Floor(config)# interface gi0/1

Floor(config-if)# description Connects to the Registrar LAN

Floor(config-if)# ip address 10.118.63.65 255.255.255.0

Floor(config-if)# no shutdown

Floor(config-if)# interface gi0/0

Floor(config-if)# description Connects to the Manager LAN

Floor(config-if)# ip address 10.118.62.196 255.255.255.0

Floor(config-if)# no shutdown

Floor(config-if)# interface s0/0/0

Floor(config-if)# description Connects to the ISP

Floor(config-if)# ip address 10.62.63.254 255.255.255.0

Floor(config-if)# no shutdown

Floor(config-if)# interface s0/0/1

Floor(config-if)# description Connects to the Head Office WAN

Floor(config-if)# ip address 209.165.200.87 255.255.255.0

Floor(config-if)# no shutdown

Floor(config-if)# end
```

- 10.118.62.196
- 10.118.62.1
- 10.62.63.254
- 209.165.200.87
- 10.118.63.65

100%

You have scored 100%.

Congratulations, you have passed the exam.

You have used 1 of 1 attempt(s).

Review assessment

Here is how you performed in each of the Learning Objectives and Skills associated with this assessment.

Basic Device Management. Initial Device Config. CLI
100%

Network Basics. Protocols. Network Layer
100%

Network Basics. Communications. ARP
100%